International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 201-208
© TJPRC Pvt. Ltd.

IMPLIMENTATION OF AN EFFICIENT MECHANISM FOR SECURE AUTHENTICATION

SHRIKALA M. DESHMUKH[1] & P. R. DEVALE[2]

[1]Research Scholar, College of Engineering, Bharati Vidyapeeth University, Pune, India

[2]Head of Information Technology Department, College of Engineering, Bharati Vidyapeeth University, Pune, India

ABSTRACT

In this paper we implemented a graphical authentication system which overcomes all drawbacks of existing authentication system. In this system we combine the features of D´ej`a Vu, Cued Click Points, Secret Draw technique and Text Passwords. In this system we used database of 20 images. In the password creation process, we provide 4 images randomly amongst database of 20 images. On first 3 images user can select click points and add single digit/text on that images. On the fourth image user draws a Secret and should add single text/digit. After password creation, for login user should correctly identify the images, correct click points, text/digit entered on that images and correct secret on correct image. This system is hard for attackers to break because if any click point, text/digit, secret is incorrect then the message of authentication fails is given after last image. So this method provides higher security than existing methods.

KEYWORDS: Authentication, Graphical Passwords, Security

INTRODUCTION

Now graphical passwords are used as an alternative to text based passwords but in this system we combined graphical passwords with text passwords. We kept graphical passwords as a base and add text passwords to it. In this graphical authentication system we combine some features of existing systems such as we took feature of D´ej`a Vu that is "Identification of images sequentially from database". We took feature of Cued Click Points that is "Message of authentication failed is given after the last click". We took feature of Secret Draw Technique that is "To Draw a Secret on a image". We took feature of Text passwords that is "To Enter text/digit".

At first we are providing a user form. This is Existing User Login form. If user has already created his/her password then he/she should login through this form. If not then user should enter on "New User Registration" process. When user fills all his/her information and press the "Show Images" button then system will display 4 images . Amongst these 4 images, On first 3 images user has decided its click point and along with click point user has to enter single text or digit at click point. On the last image, user can draw a secret and also enters single text/digit on that image. This is the password creation process. After password creation, user has to click on "save" button, through which your password and username is saved to system.

After password creation, the new user becomes existing user. Then for successful login, user has to visit Existing User form. Then user has to enter his/her name and has to press "Show Images" button. At first user has to identify these 4 images on which password is created amongst the database. After that, User has to identify first image, click point on that image and entered text/digit on that image. Then user has to select that images, click on that particular point and has to enter correct text/digit at that point.

Then user has to follow same procedure for second and third image. And on the fourth image user has to draw correct secret and he/she should identify correct text/digit on that image.

If user identifies all images, enter correct click points, enter correct text/digit and draw correct secret then user will successfully authenticate to the system.

The message of “Successful Authentication” or “Authentication Failed” is given after the last click

BACKGROUND

Some of the previously introduced Graphical Password techniques are given below,

Pass-Point Scheme

S. Wiedenbeck et al. [6][8][9] proposed pass-point scheme in which password consists of a sequence of 5 different click points on single image. In the password creation process user selects 5 pixels in an image as a click-points and for login user has to enter these clicks in correct sequence.

The two major disadvantages of pass-point systems are: 1. The problem with pass-point scheme is the HOTSPOTS [11][12](the area of an image where possibility of click-point selection is more) 2.It is easy for attackers to guess the password

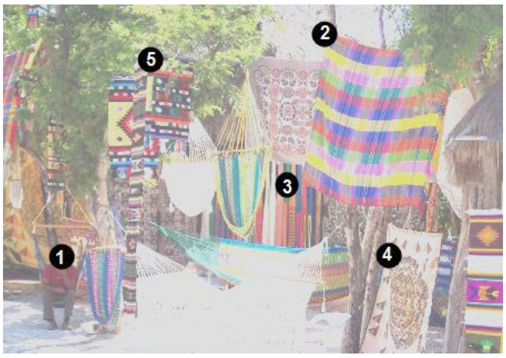


Figure 1: Pass-Points [10]

Cued Click Points

Cued Click Points [1][2] [15] mainly designed for 2 things:

- To reduce patterns[13][14] and
- To reduce the usefulness of HOTSPOTS[11][12] for attackers.

Instead of five click-points on single image, Cued Click Points [1][2] [15] uses the technique in which user has to select one click-point on five different images. The next image displayed is mainly depends on the location of the last entered click-point,it creates a path through an image database. Creating a new password with different click-points results in a different image sequence.

One best feature of Cued Click Point [1][2] [15] is that the indication message of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks[1][2] [15] .

But this technique has some disadvantages: 1. False Accept (the incorrect click point can be accepted by the system)and

- False Reject (the click-point which is correct can be rejected by the system).

- In this system, HOTSPOT remains an issue because users are selecting their own click-points [10].

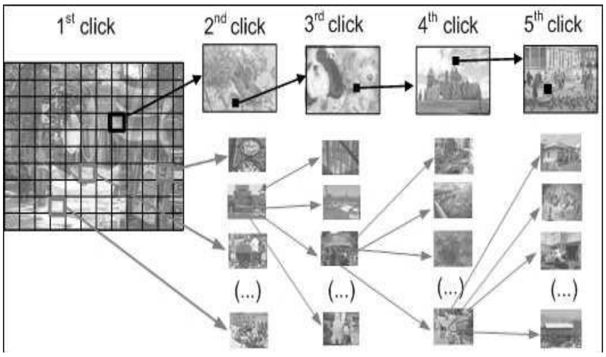
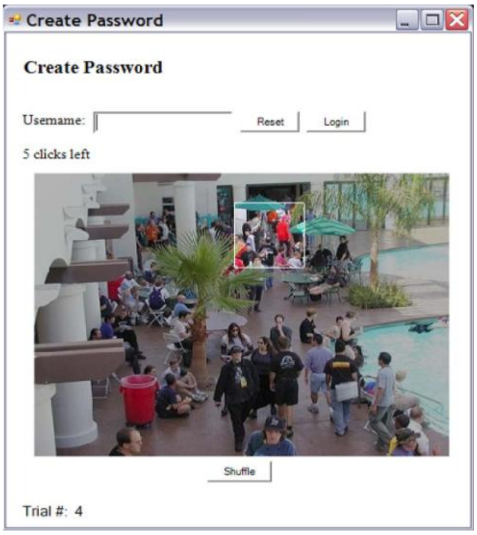


Figure 2: Cued Click Points [2]

Persuasive Cued Click Points

In creation of Persuasive Cued Click Points [1] persuasive feature is added to CCP[1][2] [15].PCCP [1] motivates users to select less predictable passwords. Terms like viewport & shuffle used in the process of password creation. It is shown in the figure that images are slightly shaded except the viewport [1] in password creation process. For avoiding known HOTSPOTS [11][12] the viewport[1] is positioned randomly].At the time of password creation users may shuffle as often as desired but it slows the process of password creation. PCCP is a good technology but has security problems. Figure shows the password creation process, viewport & shuffle button are also shown.



Create Password

Username:

5 clicks left

Trial #: 4

Figure 3: Password Creation in PCCP. Highlighted Area is Viewport (Pool Image is Taken from [16], [1]

CLICK-DRAW BASED GRAPHICAL PASSWORD SCHEME

The purpose of click-draw based graphical password scheme (*CD-GPS*)[3] is to provide both security and usability. There are mainly two steps in this scheme:

1. Image selection

2. Secret drawing.

Image Selection

In *CD-GPS[3]*, the first step is the *image selection. I*n first step users select several images from an image pool.

Suppose there are $N1$ images in the image pool, then at first users should select $n \in N1$ images from the image pool in a order and remember this order of images. Users may choose $k \in n$ image from the above selected n images. k is nothing but the single image on which we have to draw secret.[3]

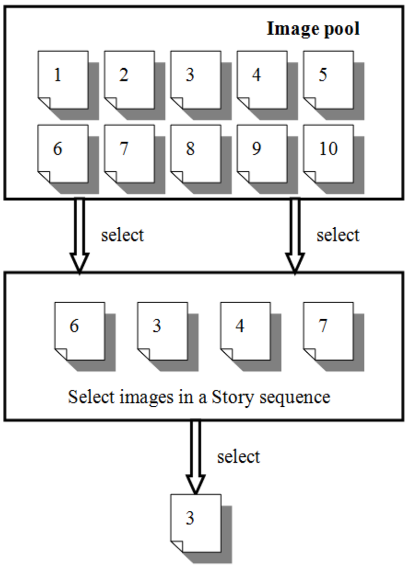


Figure 4: Image Selection in Click Draw Based Graphical Password Scheme[3]

As shown in Figure, there are total 10 images in the image pool i.e.N1 images. User first selects 4 images from the image pool in a sequence i.e. n images (e.g., {6, 3, 4, 7}).Then user selects 1 image i.e. k image (e.g., {3}) from n to draw the secret.

Secret Drawing

This is the second step comes after the image selection. In this step users can freely click-draw their secrets. For constructing secret drawing users use series of clicks. The figure is divided into a 16×16 table. Users can use the coordinate numbers for remembering their drawings. In above figure. user draw letter “T” as the secret, which covers the coordinates of (13, 3), (13, 4), (13, 5), (14, 4), (15, 4).In this technique there is not necessity to remember the sequence [3].

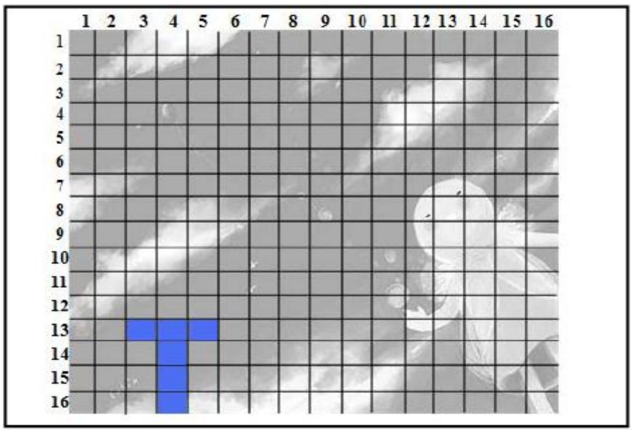


Figure 5: User Draw Letter “T” as the Secret [3]

EXPERIMENTAL WORK /RESULTS

At first we are providing a user form. This is Existing User Login form. If user has already created his/her password then he/she should login through this form.

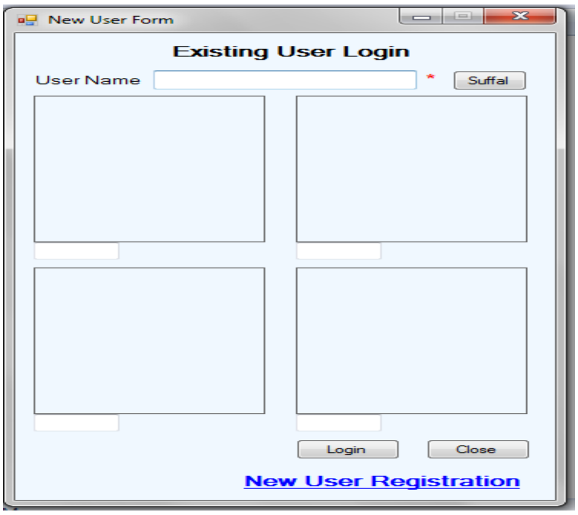


Figure 6: User Login Form

If user is new he/she should go through “New User Registration” process. When user clicks on “New User Registration” then following form will display.

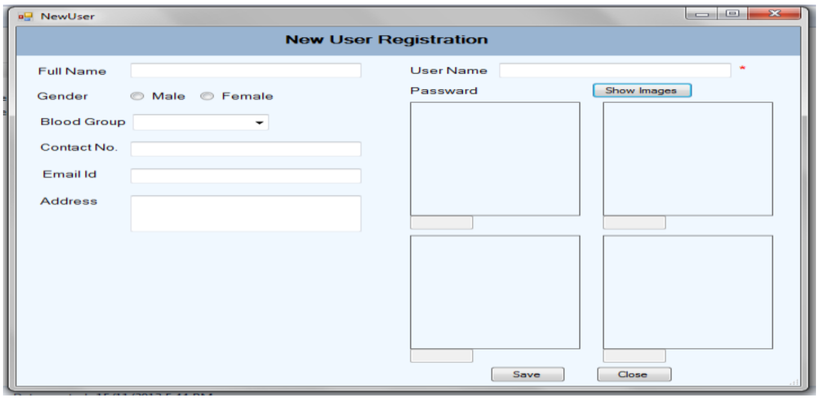
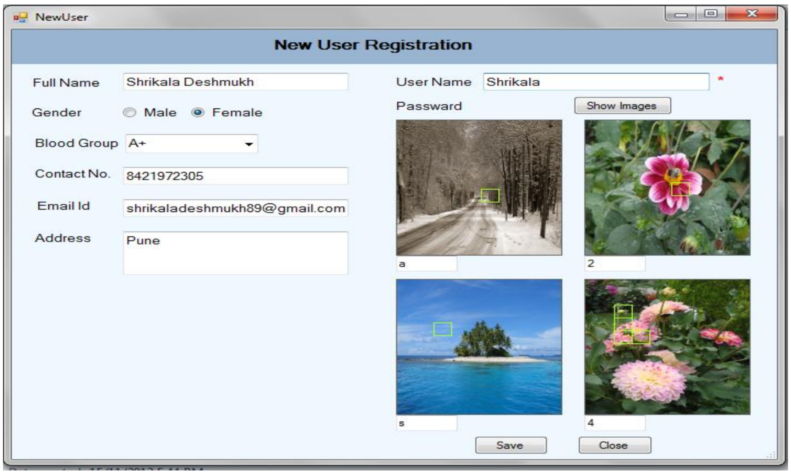


Figure 7: New User Registration Form

When user fills all his/her information and press the “Show Images” button then 4 images will display. It is shown in following figure



Full Name Shrikala Deshmukh

Gender ○ Male ● Female

Blood Group A+

Contact No. 8421972305

Email Id shrikaladeshmukh89@gmail.com

Address Pune

User Name Shrikala *

Passward

a

2

s

4

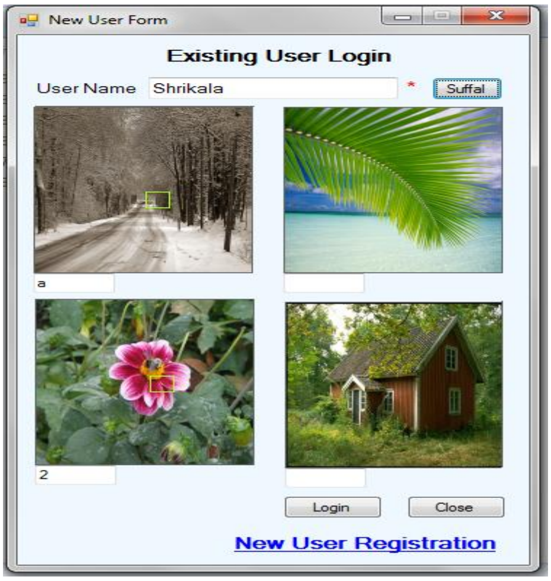
Figure 8: Password Creation Process in New User Registration Form

In above figure user fills all his/her information and created his/her password. On first 3 images

User selects his/her click points and enters single digit/text at the place of click and on the last image user draws a secret and should insert single text/digit on that image. After creating password user has to click on “Save” button.

The process of password creation is completed here. After creating password successfully, user has to identify all images, correct click points, text/digit entered at click points and correct secret on specified image.

When user clicks on “Next” button,4 images will display. Then user has to identify his/her first image amongst the database of 20 images. After identifying first image user has to identify his/her correct click point and correct text/digit on that image. User has to repeat same procedure for second image .In this following figure we shows that user identifies first and second image, correct click point on that images and correct text/digit at the click points


New User Form

Existing User Login

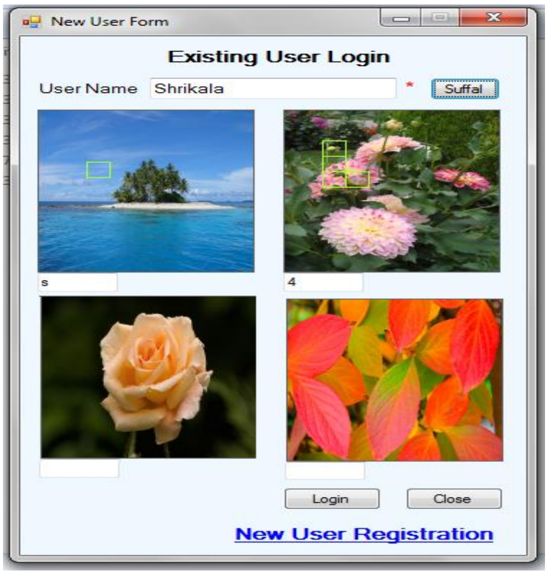
User Name Shrikala *

a

2

Figure 9: Password Identification Process

After identifying 2 images, user has to click on “Next” button for seeing various images from database. When he/she press “Next ” button, another 4 images from database will display .In following figure, user identifies third image correct click point on that image and correct text/digit on that image. User also identifies fourth image,correct secret on that image and correct text/digit on that image.


New User Form

Existing User Login

User Name Shrikala *

s

4

Figure 10: Password Identification Process

At the last user has to press “Login” button. If user identifies all images, correct click points, correct text/digit and correct secret then user will successfully authenticate to the system. When user fails to identify any image, click point ,text/digit and secret then the message of “Authentication Failed” is given after the last step.

Here we shown comparison of our system with existing systems using graphs

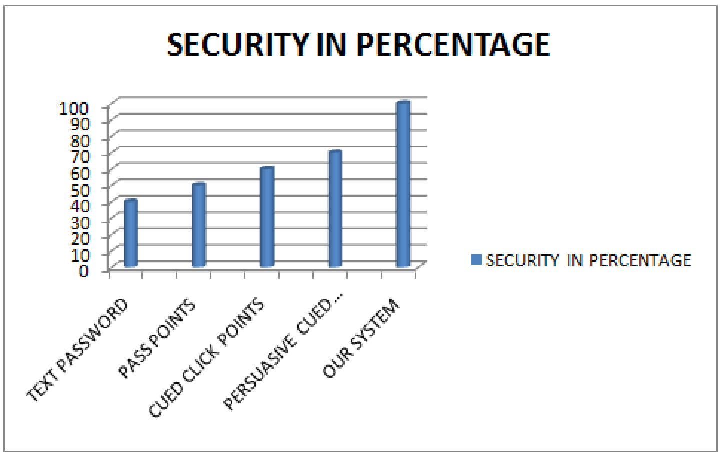


Figure 11

CONCLUSIONS

In this paper we implemented a idea of combining features of D´ej`a Vu, Cued Click points, Text passwords and Secret Drawing. By combining these features our system provide higher security and usability. Our system is very hard for attackers to break because attackers can’t guess click points, text/digit and secret are combined in a system. And it is hard to identify images from database on which user created a password and the image on which secret is drawn by user. It is also very hard for attackers to correctly identify the images, correct click points, text/digit and secret .Since our system overcomes all drawbacks of existing systems, it is very much useful and gives higher security than other systems.

REFERENCES

1. Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget,Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE “Persuasive Cued Click Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012

2. Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle2“Graphical Password Authentication Using Cued Click Points”1 School of Computer Science, Carleton University, Ottawa, Canada.2 Human-Oriented Technology Lab, Carleton University, Ottawa, Canada(chiasson,paulv)@scs.carleton.ca, robert biddle@carleton.ca

3. Yuxin Meng “Designing Click-Draw Based Graphical Password Scheme for Better Authentication” 2012 IEEE Seventh International Conference on Networking, Architecture, and Storage

4. Karen Renaud*a Department of Computing Science, University Of Glasgowkaren@dcs.gla.ac.uk* “Quantifying the Quality of Web Authentication Mechanisms A Usability Perspectivity “Journal of Web Engineering, Vol. 0, No. 0 (2003) 000–000_c Rinton Press.

5. Nelson, D.L., U.S. Reed, and J.R. Walling. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, 485-497, 1977.

6. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. “PassPoints:Design and longitudinal evaluation of a graphical password system”. International Journal of Human Computer Studies, 2005.

7. I.Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. Proceedings of the Eighth USENIX Security Symposium,pages 1–14, 1999.

8. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Authentication Using Graphical Passwords: Effects of Toler-ance and Image Choice,” *Proc. First Symp. Usable Privacy and Security (SOUPS),* July 2005.

9. Dirik, N. Menon, and J. Birget, “Modeling User Choice in the Passpoints Graphical Password Scheme,” *Proc. Third ACM Symp. Usable Privacy and Security (SOUPS)*, July 2007.

10. Ms. Uma D.Yadav and Mr. P. S. Mohod,“Enhancement of Knowledge Based Authentication Mechanism using Graphical Password via Persuasion” JOURNAL OF COMPUTER SCIENCE AND ENGINEERING, VOLUME 17, ISSUE 2, FEBRUARY 2013

11. K. Golofit, “Click Passwords under Investigation,” Proc. 12th European Symp. Research in Computer Security (ESORICS), Sept.2007.

12. A. Dirik, N. Menon, and J. Birget, “Modeling User Choice in the Passpoints Graphical Password Scheme,” Proc. Third ACM Symp.Usable Privacy and Security (SOUPS), July 2007.

13. S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, “User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords,” Int’l J. Information Security, vol. 8, no. 6, pp. 387-398, 2009.

14. A. Salehi-Abari, J. Thorpe, and P. van Oorschot, “On Purely Automated Attacks and Click-Based Graphical Passwords,” Proc. Ann. Computer Security Applications Conf. (ACSAC), 2008.

15. S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical Password Authentication Using Cued Click Points,” Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

16. PD Photo, PD Photo Website, http://pdphoto.org, Feb. 2007.

17. J. Yan, A. Blackwell, R. Anderson, and A. Grant, “The Memorability and Security of Passwords,” Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O’Reilly Media, 2005.